PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 21 de marzo de 2024

070-2024-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aérea del Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y las empresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 21-03-2024
		Página: 4 de 15

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	AcidPour, la nueva amenaza dirigida a dispositivos Linux (x86)		
Tipo de Ataque	Malware	Abreviatura	Malware
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Se ha detectado en el entorno un nuevo tipo de malware destructivo llamado AcidPour, dirigido a dispositivos de red y Linux x86 IoT.

AcidPour es un tipo de malware categorizado como "borradores de datos", diseñados para realizar ataques que eliminan archivos y datos en dispositivos específicos. Se utilizan con frecuencia para interrumpir las operaciones de una organización o a modo de distracción durante un ataque más amplio.

También se les conoce como “wiper” (en inglés, “borrador” o “limpiador”) es un tipo de software malicioso diseñado para dañar o destruir información en un sistema informático. A diferencia de otros tipos de malware que buscan robar información o infectar sistemas con fines lucrativos, el objetivo principal del wiper es eliminar datos y archivos del sistema de manera irreparable.

AcidPour es una variante destructiva del malware AcidRain. Fue visto por primera vez en Ucrania y descubierto el 16MAR2024 por Tom Hegel de SentinelOne.

El 24 de febrero de 2022, un ciberataque dejó inoperables los módems Eutelsat KA-SAT en Ucrania. El efecto de este ataque hizo que 5.800 turbinas eólicas de Enercon en Alemania no pudieran comunicarse para su monitoreo o control remoto y, según se informa, afectó servicios vitales en toda Europa.

El 30 de marzo de 2022, se identificó un componente de limpieza al que se denominó 'AcidRain' como parte de la cadena de ataque que causó esta interrupción.

Se evaluó con confianza media que existen similitudes de desarrollo entre AcidRain y un complemento destructivo de etapa 3 de VPNFilter llamado 'dstr'.

El 16 de marzo de 2024, observamos un nuevo limpiador de Linux al que llamamos 'AcidPour'. Alertamos a los socios relevantes de inmediato para frenar el potencial de cualquier impacto regional significativo adicional, seguido de la difusión pública de indicadores técnicos y análisis tempranos para alertar a la comunidad de investigación y fomentar la vigilancia y las contribuciones.

2. DETALLES:

Mientras que AcidRain es un limpiador de Linux compilado para la arquitectura MIPS para compatibilidad con los dispositivos de destino, AcidPour está compilado para la arquitectura x86. A pesar de que ambos apuntan a sistemas Linux, la discrepancia en la arquitectura limita de alguna manera nuestra capacidad para comparar las bases de código compiladas.

Nuestro análisis técnico sugiere que las capacidades ampliadas de AcidPour le permitirían deshabilitar mejor los dispositivos integrados, incluidas redes, IoT, almacenamiento grande (RAID) y posiblemente dispositivos ICS que ejecutan distribuciones Linux x86.

La variante AcidPour es un binario ELF compilado para x86 (no MIPS) y, si bien se refiere a dispositivos similares, el código base se ha modificado y ampliado para incluir capacidades adicionales. Los mejores intentos automatizados de comparar diferentes arquitecturas solo arrojan una confianza baja, menor al 30% de similitud.

Las similitudes notables incluyen el uso del mismo mecanismo de reinicio, la lógica exacta de la limpieza recursiva del directorio y, lo más importante, el uso del mismo mecanismo de limpieza basado en IOCTL utilizado tanto por AcidRain como por el complemento VPNFilter 'dstr'.

AcidPour está diseñado para borrar contenido de matrices RAID y sistemas de archivos de imágenes de bloques sin clasificar (UBI) mediante la adición de rutas de archivos como "/dev/dm-XX" y "/dev/ubiXX", respectivamente, que sugieren un enfoque en sistemas embebidos, sistemas que usan memoria flash y gestión de volúmenes lógicos, y dispositivos de almacenamiento conectados a la red. Los dispositivos de almacenamiento en red, como QNAP y Synology, utilizan LVM para gestionar matrices RAID.

AcidPour está programado en C sin depender de librerías compiladas estáticamente o importaciones. La mayor parte de la funcionalidad se implementa a través de llamadas directas al sistema, muchas de ellas mediante el uso de ensamblador en línea y opcodes.

Al incluir la lógica UNSORTED BLOCK IMAGE (UBI) y DEVICE MAPPER (DM), AcidPour, amplia la cantidad de dispositivos que podían ser afectados originalmente por AcidRain.

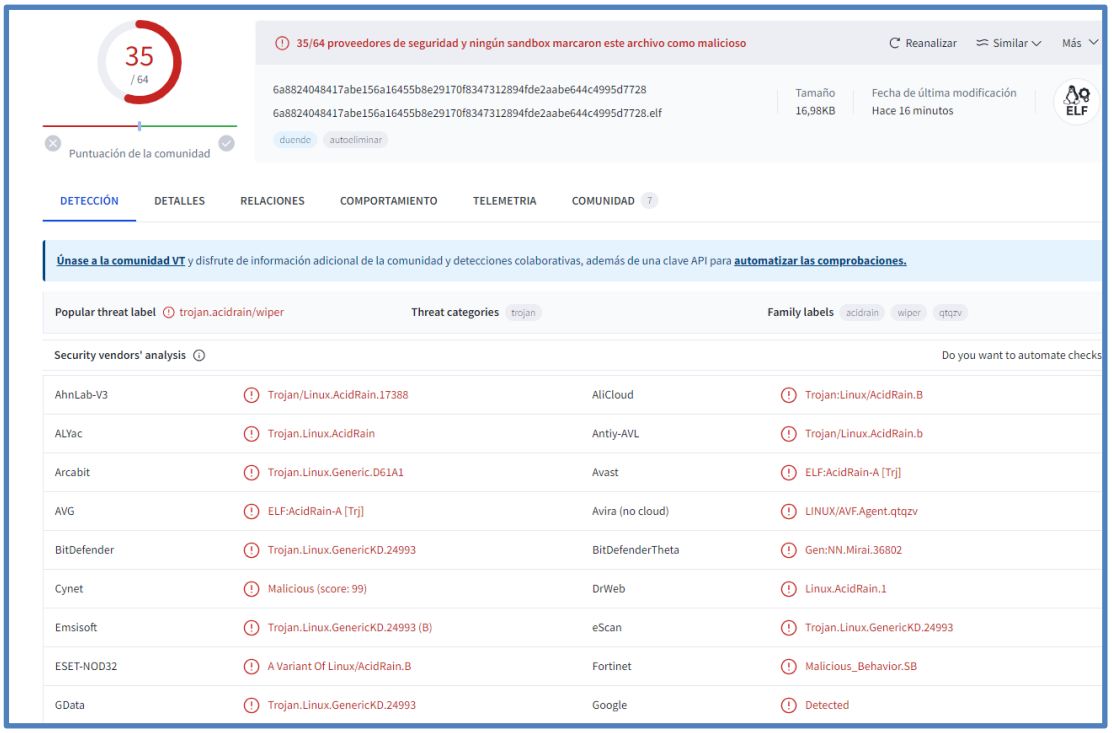
El equipo de SentinelLabs ha compartido el hash del malware, invitando a la comunidad de investigación de seguridad a colaborar en su análisis y validación, dada la incertidumbre actual sobre sus objetivos y alcance de distribución.

La repetición de la sugerencia de que AcidPour podría afectar a una diversidad mayor de dispositivos resalta la gravedad de esta amenaza. Rob Joyce, director de ciberseguridad de la NSA, expresó su preocupación, calificando a esta variante como una versión más poderosa de AcidRain, capaz de comprometer una gama más extensa de hardware y sistemas operativos.

IoCs:

IPs:

- 185.125.188[.]58
- 185.125.188[.]59
- 38.100.168[.]192



HASH:

- MD5: 1bde1e4ecc8a85cffef1cd4e5379aa44
- SHA1: b5de486086eb2579097c141199d13b0838e7b631
- SHA256: 6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728

Nombre del archivo: '/tmp/tmphluyl8zn'

Dispositivos compatibles con AcidPour:

- /dev/loop/* Virtual Block Devices
- /dev/block/mmcblk* Acceso a tarjetas SD/MMC.
- /dev/mtd* Dispositivo o memoria flash que permite fileops
- /dev/block/mtdblock* Memoria Flash
- /dev/mtdblock* Memoria Flash (común en routers e IoT)
- /dev/sd* Dispositivo genérico

3. RECOMENDACIONES:

- Actualizar el software de los dispositivos de red a la última versión.
- Implementar la autenticación multifactor (MFA) en todos los sistemas y cuentas críticas.
- Mantener actualizado el software y los parches de seguridad.
- Realizar Copias de Seguridad efectivas y regulares, almacenadas de manera segura y separada de la red principal.
- Fortalecer las políticas de contraseñas y realizar auditorías de seguridad regulares.
- Implementar soluciones de seguridad tales como firewalls, sistemas de detección de intrusiones, EDR y de copia de seguridad robustas.
- Mantener un nivel proactivo de monitoreo y búsqueda de amenazas.
- Disponer de servicios que brinden la alerta temprana y búsqueda de amenazas en la red; tales como el Data Risk Protection, Cyber Intelligence y ThreatHunting.

Fuente de Información:	• hxxps://ciberprisma.org/2024/03/19/acidpour-la-nueva-amenaza-dirigida-a-dispositivos-linux-x86/ • hxxps://blog.tecnetone.com/acidpour-nuevo-malware-amenaza-dispositivos-de-red-linux-x86 • hxxps://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/ • hxxps://www.linuxsc.net/se-sospecha-que-el-malware-ruso-acidpour-borra-datos-esta-dirigido-a-dispositivos-linux-x86/ • hxxps://thehackernews.com/2024/03/suspected-russian-data-wiping-acidpour.html • hxxps://www.bleepingcomputer.com/news/security/new-acidpour-data-wiper-targets-linux-x86-network-devices/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070**	**Fecha: 21-03-2024**
		Página: 7 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en la interfaz de administración de Kemp LoadMaster de Progress		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección de comando del sistema operativo en la interfaz de administración de Kemp LoadMaster. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto elevar privilegios y la ejecución arbitraria de comandos del sistema.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-1212 de tipo inyección de comando del sistema operativo en el equilibrador de carga Progress Kemp LoadMaster, podría permitir la inyección de comandos no autenticados en la interfaz web del administrador. Un atacante remoto no autenticado podría acceder al sistema a través de la interfaz de administración de LoadMaster, lo que permite la ejecución arbitraria de comandos del sistema.

Progress Software Corporation, indica que ha parcheado esta vulnerabilidad crítica, pero antes de la solución, los actores de amenazas podrían haber explotado esta vulnerabilidad para obtener acceso no autorizado a los sistemas afectados.

Progress indico que se ha publicado un script de Python diseñado como prueba de concepto (PoC) para demostrar la explotación de la vulnerabilidad de tipo inyección de comandos no autenticados en Kemp LoadMaster, identificada como CVE-2024-1212.

A. Productos afectados:

- LoadMaster, afectado desde la versión 7.2.48.1 antes de 7.2.48.10.
- LoadMaster, afectado desde la versión 7.2.54.0 antes de 7.2.54.8.
- LoadMaster, afectado desde la versión 7.2.55.0 antes de 7.2.59.2.

3. RECOMENDACIÓN:

- Aplicar los parches correspondientes para evitar posibles violaciones de seguridad y protegerse contra impactos posteriores a proveedores o tecnologías de terceros.

Fuente de Información:	• hxxps://github.com/Chocapikk/CVE-2024-1212 • hxxps://support.kemptechnologies.com/hc/en-us/articles/23878931058445-LoadMaster-Security-Vulnerability-CVE-2024-1212 • hxxps://support.kemptechnologies.com/hc/en-us/articles/23878931058445-LoadMaster-Security-Vulnerability-CVE-2024-1212

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 21-03-2024
		Página: 8 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en la configuración de Apache Commons		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **ALTA** de tipo escritura fuera de límites en la configuración de Apache Commons. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario y comprometer el sistema.

2. DETALLES:

Apache Commons es un proyecto de software de la Apache Software Foundation que proporciona una biblioteca de componentes reutilizables para diversas tareas de programación en Java. Estos componentes abarcan áreas como colecciones, entrada/salida (I/O), concurrencia, matemáticas, entre otros.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-29131 de tipo escritura fuera de límites, existe debido a un error de límite al procesar entradas que no son de confianza. Un atacante remoto puede pasar datos especialmente diseñados a la aplicación, provocar una escritura fuera de límites y ejecutar código arbitrario en el sistema objetivo.

A. Productos afectados:

- Apache Commons Configuration: 2.0 - 2.10.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://seclists.org/oss-sec/2024/q1/239

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070**	**Fecha: 21-03-2024**
		Página: 9 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en SCAN_VISIO eDocument Suite Web Vierwer de Abast		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo inyección SQL en SCAN_VISIO eDocument Suite Web Vierwer de Abast. La explotación exitosa de esta vulnerabilidad podría permitir a un usuario no autenticado, recuperar, actualizar y eliminar toda la información de la base de datos.

2. DETALLES:

SCAN_VISIO eDocument Suite Web Viewer de Abast es una solución de visualización de documentos web desarrollada por la empresa Abast, especializada en tecnología de gestión documental. Esta suite proporciona herramientas avanzadas para visualizar diversos tipos de documentos directamente en un navegador web, lo que facilita el acceso y la colaboración en documentos almacenados en sistemas de gestión documental compatibles.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-29732 de tipo inyección SQL, permite a un usuario no autenticado, recuperar, actualizar y eliminar toda la información de la base de datos. Esta vulnerabilidad se encontró en la página de inicio de sesión mediante el parámetro "user".

A. Productos afectados:

- SCAN_VISIO Web Viewer, versión 3.28.1 e inferiores.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://www.abast.es/automatizacion-de-procesos-y-rpa/scan_visio-edocument-suite/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070**	**Fecha: 21-03-2024**
		Página: 10 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en el registrador de fallas digital Elspec G5		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Se ha reportado múltiples vulnerabilidades de severidad **ALTA** de tipo desbordamiento de búfer, uso de credenciales codificadas, recorrido de camino, permisos privilegios y controles de acceso, inclusión de información confidencial en archivos de registro y divulgación de información en el registrador de fallas digital Elspec G5. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto ejecutar código arbitrario en el sistema de destino, realizar ataques de cruce de directorios, escalar privilegios y obtener acceso a información confidencial.

2. DETALLES:

Elspec G5 es un tipo de analizador de calidad de energía eléctrica fabricado por la empresa Elspec Ltd. Este dispositivo se utiliza para monitorear y analizar la calidad de la energía eléctrica en diferentes entornos, como instalaciones industriales, comerciales y de servicios públicos. El G5 es conocido por su capacidad para detectar y analizar armónicos, flicker, desequilibrios de tensión y otros problemas de calidad de la energía. Es una herramienta importante para asegurar el funcionamiento óptimo de los sistemas eléctricos y para identificar posibles problemas que puedan afectar la operación de equipos sensibles o causar interrupciones en el suministro eléctrico.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-22080 de tipo desbordamiento de búfer, existe debido a un error de límite durante el análisis del cuerpo XML. Un atacante remoto puede provocar daños en la memoria y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-22081 de tipo desbordamiento de búfer, existe debido a un error de límite en el mecanismo de análisis del encabezado HTTP. Un atacante remoto puede provocar daños en la memoria y ejecutar código arbitrario en el sistema de destino.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-22083 de tipo uso de credenciales codificadas, existe debido a la presencia de una ID de sesión de puerta trasera codificada. Un atacante remoto no autenticado puede acceder al sistema afectado utilizando las credenciales codificadas.

Se han asignado los siguientes identificadores para las vulnerabilidades de severidad **media**: CVE-2024-22079, CVE-2024-22077, CVE-2024-22084, CVE-2024-22085, CVE-2024-22082, y CVE-2024-22078

A. Productos afectados:

- G5 digital fault recorder: 1.1.4.15.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxp://www.elspec-ltd.com/support/security-advisories/

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070**	**Fecha: 21-03-2024**
		Página: 11 de 15

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Actualizaciones recientes de Windows Server provocan reinicios y bloqueos en el controlador de dominio debido a la pérdida de memoria LSASS		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Múltiples usuarios han reportado que las actualizaciones acumulativas de marzo de 2024 para Windows Server 2016 y Windows Server 2022 (KB5035855 y KB5035857), están provocando reinicios y bloqueos de los controladores de dominios. La pérdida de memoria en el Servicio del Subsistema de Autoridad de Seguridad Local (LSASS) introducida por las actualizaciones es la causa directa de los fallos y reinicios, esto provoca interrupciones en las operaciones comerciales normales y crea un riesgo para la seguridad de la red y la integridad de los datos.

2. DETALLES:

El problema de se debe a una pérdida de memoria LSASS, un componente crítico del sistema operativo Windows responsable de hacer cumplir las políticas de seguridad y administrar los inicios de sesión de los usuarios, la creación de tokens de acceso y los cambios de contraseñas.

Cabe señalar, que el proceso LSASS es esencial para el funcionamiento estable de los controladores de dominio, que son fundamentales en la gestión de la seguridad de la red y la autenticación de usuarios dentro del entorno de TI de una organización.

Las recientes actualizaciones acumulativas de marzo de 2024 para Windows Server 2016 y Windows Server 2022 se han relacionado con importantes interrupciones en la infraestructura de TI, con numerosos reportes de controladores de dominio que experimentaron fallas y reinicios forzados.

Los administradores que han reportado las fallas, han indicado que los controladores de dominio muestran un uso de memoria LSASS en constante aumento después de instalar las actualizaciones de marzo. Este aumento en el consumo de recursos casualmente hace que el sistema deje de responder, lo que genera fallas y reinicios automáticos, provocando interrupciones en las operaciones comerciales normales y crea un riesgo para la seguridad de la red y la integridad de los datos.

La pérdida de memoria LSASS introducida por las actualizaciones es la causa directa de los fallos y reinicios. Las pérdidas de memoria ocurren cuando un programa administra incorrectamente las asignaciones de memoria, lo que reduce el rendimiento y la estabilidad del sistema a medida que la memoria disponible se agota gradualmente. En el caso de los controladores de dominio, la pérdida de memoria del proceso LSASS provoca una carga insostenible en el sistema, lo que obliga a un bloqueo como último recurso para recuperarse del fallo.

A. Productos afectados:

- Windows Server 2016.
- Windows Server 2022.

3. RECOMENDACIONES:

- Revertir las actualizaciones mencionadas.
- Actualizar los paquetes afectados cuando Microsoft lance una última versión que aborde estas vulnerabilidades. Actualmente aún no hay ninguna solución oficial.
- Realizar pruebas exhaustivas y garantizar la calidad en las actualizaciones de software, principalmente cuando afectan componentes críticos de la infraestructura de TI empresarial.

Fuente de Información:	• hxxps://gbhackers.com/windows-server-updates-trigger-domain-controller-failures-and-reboots/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°070	Fecha: 21-03-2024
		Página: 12 de 15

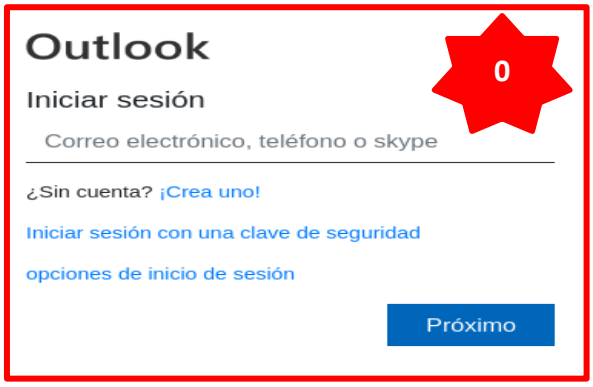
Componente que reporta	**DIRECCIÓN DE INTELIGENCIA DE LA POLICIA NACIONAL DEL PERÚ**		
Nombre de la alerta	Nueva campaña de Phishing que suplanta la identidad de Microsoft Outlook		
Tipo de Ataque	Phishing	Abreviatura	Phishing
Medios de propagación	Redes sociales, SMS, correo electrónico, videos de internet, entre otros		
Código de familia	G	Código de Sub familia	G01
Clasificación temática familia	Fraude		

Descripción

1. **ANTECEDENTES:**

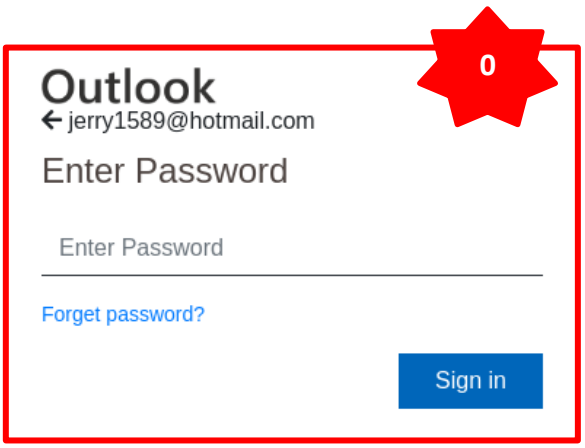
A través del monitoreo y búsqueda de amenazas en el ciberespacio, se detectó que, los ciberdelincuentes se encuentran desarrollando una campaña de Phishing, a través de los diferentes navegadores web, quienes vienen suplantando la identidad del sitio oficial de Microsoft Outlook, (que es un programa informático gestor de correo electrónico desarrollado por Microsoft); con el objetivo de acceder u obtener credenciales de inicio de sesión de las posibles víctimas.

2. **DETALLES:**



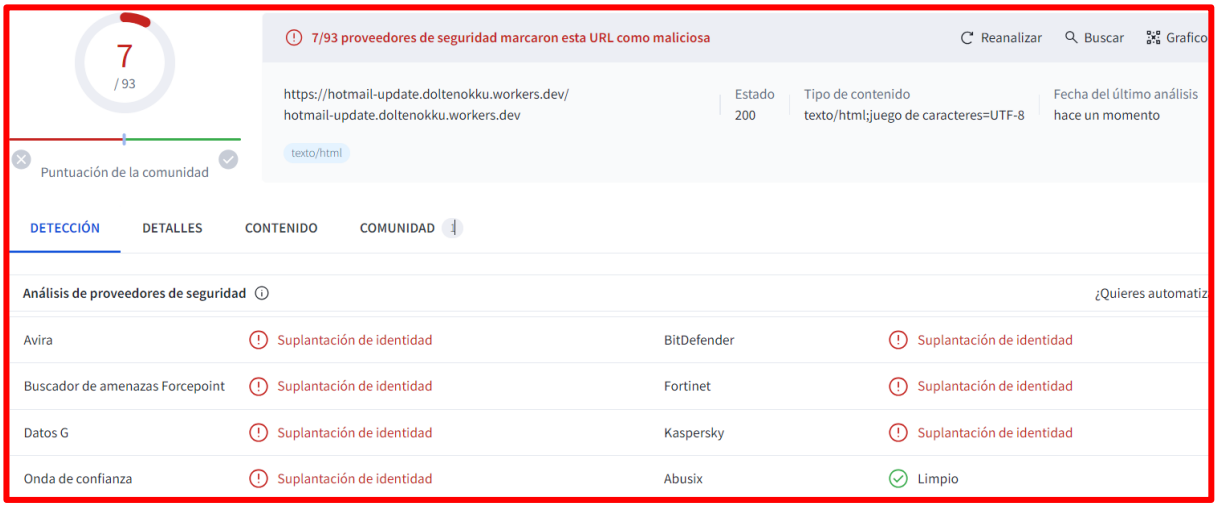
Sitio web fraudulento de la corporación tecnológica de Microsoft Outlook, solicita a la víctima que registre el correo electrónico, el teléfono o skype, para poder continuar.

Luego de registrar el correo electrónico, el atacante le solicita a la víctima que registre la contraseña para poder ingresar.



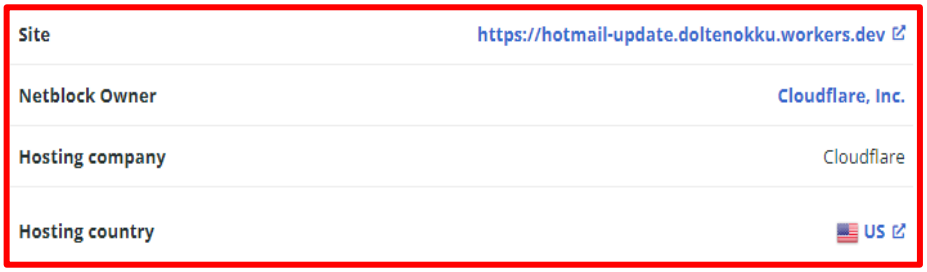
Al registrar las credenciales de acceso, es redirigido al sitio web oficial del sitio web de Microsoft; sin embargo, los ciberdelincuentes obtuvieron los datos proporcionados por la víctima.

A. La URL Maliciosa, fue analizada en las diferentes plataformas virtuales de seguridad digital, siendo catalogado como **SUPLANTACIÓN DE IDENTIDAD:**

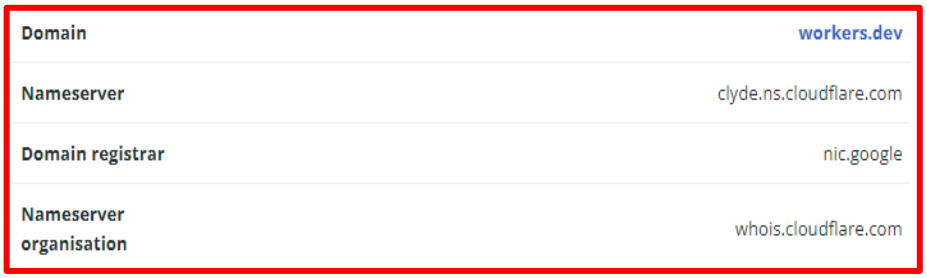


B. Indicadores de compromisos:

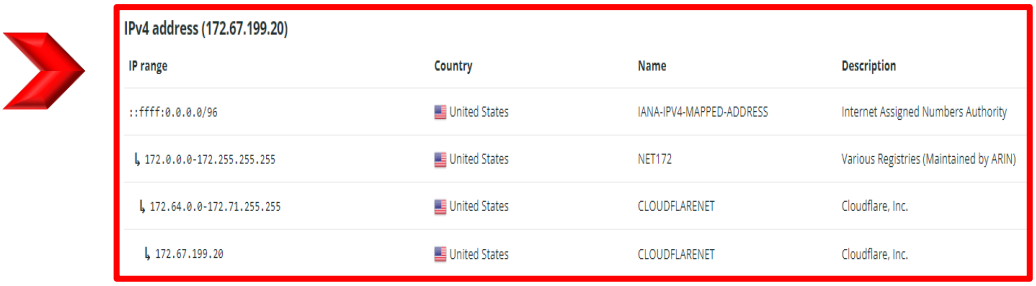
I. URL: hxxps[:]//hotmail-update[.]doltenokku[.]workers[.]dev



II. DOMINIO: workers[.]dev



III. IP: 172[.]67[.]199[.]20



IV. SHA-256: 0bac060a8a6245abfcfeaa1d330a907dd5b9e1f73f919eeacf089163c4599938

V. Servidor: Cloudflare

C. Cómo funciona el Phishing:

- Los correos electrónicos incluyen enlaces a sitios web preparados por los ciberdelincuentes en los que solicitan información personal.
- Medios de propagación del Phishing: WhatsApp, Telegram, redes sociales, SMS entre otros.
- Los ciberdelincuentes intentan suplantar a una entidad legitima (organismo público o privado, entidad financiera, servicio técnico, etc.)

D. Referencia:

- Phishing o suplantación de identidad: Es un método que los ciberdelincuentes, utilizan para engañar a los usuarios para conseguir que revele información personal, como contraseñas, datos de tarjetas de créditos, números de cuentas bancarias, entre otros.

3. RECOMENDACIONES:

- Evitar acceder a enlaces que llegan inesperadamente por correo electrónico u otros medios.
- No proporcionar datos personales (contraseñas, tarjetas, cuentas bancarias, etc.) por correo, teléfono o SMS.
- No introducir datos confidenciales en sitios web sospechosas o de dudosa procedencia.
- Verificar la fuente de información de tus correos entrantes.
- Introducir tus datos únicamente en webs seguras.
- Tener siempre actualizado el sistema operativo y el antivirus. En el caso del antivirus, comprobar que está activo.

Fuente de Información:	Análisis propio de redes sociales y fuente abierta

Índice alfabético